On threats

- Cyber threats from nation states and their proxies are and will remain acute. Of particular concern to us are cyber threats to physical and digital critical infrastructure.

- These threats are not theoretical – they are reality right now. In the prosecution of its premeditated, unprovoked, and unjustified further invasion, Russia has conducted disruptive and destructive cyber attacks to undermine, coerce, and destabilize Ukraine. Victims of these cyber attacks include non-military victims like Ukrainian banks, and we have also seen disruptive cyber attacks against government websites and other private sector entities.

- Compared to other capabilities, cyber tools are relatively low cost and widely available. An increasing number of countries and nonstate actors have advanced cyber capabilities, including those supplied by private companies, which can achieve high impact and even strategic-level effects.

- Some states refuse to acknowledge their own national cyber capabilities while criticizing nations that are more transparent. Transparency in this respect is useful in fostering communication between states that can help avoid misunderstanding and escalation. Evasiveness or lack of transparency about national cyber capabilities, on the other hand, is more likely to increase instability between states.

- As states attempt more significant cyber operations, they risk causing harm to civilian populations. Their actions may also embolden other states to engage in similarly unbridled activity. In addition, irresponsible cyber behavior by one state could
undermine international norms and result in greater instability for all nations.

- In the midst of the COVID pandemic, we have also grown more aware of the range of cyber risks to the health sector, particularly to medical devices or vaccine research trials where a relatively minor disruption or manipulation of data could cause loss of life. Similarly, ransomware attacks on medical facilities have the potential to threaten lives or undermine the provision of necessary medical treatments.

- The United States is concerned that – despite internationally-recognized peacetime norms of responsible state behavior - several advanced adversaries, capable of causing disruption, are targeting critical infrastructure, including underwater cables, oil and gas pipelines, communications networks, and rail systems, and could choose to carry out attacks with severely disruptive effects.

- For example, according to press reporting, just last month, an “external cyber event” involving a commercial satellite communication network’s ground infrastructure affected Ukrainian military communications and also disrupted tens of thousands of systems outside of Ukraine, including communications with wind turbines and individual satellite internet connections across Europe. Activity resulting in such a spillover effect is irresponsible and destabilizing, especially when carried out in a crisis environment where there is a heightened risk of escalation.

- In further evidence of potentially escalatory use of cyber capabilities, last week the U.S. Department of Justice unsealed the indictment of an employee of a Russian Ministry of Defense
research institute and his co-conspirators who are alleged to have used cyber capabilities to damage critical infrastructure outside the United States, leading to two separate emergency shutdowns at an oil refinery. These individuals were also alleged to have attempted to access the computers of a U.S. company that managed similar critical infrastructure entities in the United States.

- Separately, the Justice Department has also charged three officers of Russia’s Federal Security Service and their co-conspirators who targeted and undertook to compromise the computers of hundreds of entities related to the energy sector. This was not an espionage campaign. The sole logical reason for gaining access to such systems was to provide the Russian government the future ability to disrupt and damage critical infrastructure systems.

- In light of both historical and recent Russian cyber activity, the White House has issued an urgent warning to the U.S. private sector that the Russian government is exploring options for cyber attacks on U.S. critical infrastructure in response to the unprecedented costs the United States and its allies and partners have imposed on Russia to hold it accountable for its unprovoked attack on Ukraine.

- The United States is also concerned about the increase in global risk from cybercriminals who are allowed by certain states to operate with impunity within their territory. We have repeatedly raised the issue of cybercriminals who maintain mutually beneficial relationships with countries, including Russia, that offer them safe haven or benefit from or, in some cases, direct their activity. And we are equally perturbed that certain states allow their government cyber personnel to moonlight as cyber criminals in their spare time, potentially leveraging the government’s access
or tools to facilitate their personal cybercrime activities. Such activities could be misinterpreted, and lead to instability or confrontation.

- Finally, as we confront the threats that most concern us today, we must also look to the future and the implications of emerging technologies, such as AI, for the framework for responsible state behavior. As we do so, however, we must keep in mind that it is not the technologies themselves, but the way that these technologies may be used by States that has the potential to threaten peace and stability.

- We look forward to working with responsible UN member states to identify cyber threats of shared concern to international peace and security and to implement effective measures aimed at decreasing those risks.